

Notice of Allowability

Application No.

09/864,042

Examiner

Jung W. Kim

Applicant(s)

ANANTH, VISWANATH

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to 27 June 2005.
2. ☒ The allowed claim(s) is/are 1-24 and 30-34.
3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 - a) ☐ All b) ☐ Some* c) ☐ None of the:
 1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

* Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.

THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
 5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
 - (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
 - 1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
 - (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.
- Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____
7. ☒ Examiner's Amendment/Comment
8. ☐ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____

EXAMINER'S AMENDMENT

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with William W. Schaal on September 1, 2005.

The application has been amended as follows:

In the claims:

Claim 2, lines 3-4: replace "an internal identifier and an output of a first non-linear function." with --an internal identifier, an output of a first non-linear function and changes in the incoming plain text--.

Claim 15, lines 2-4: replace "a memory; and encryption logic to perform a stream cipher operation on input data segmented in random sized blocks forming a sequence of blocks using an encryption key, the size of each block of the sequence of blocks varying in response to changes in the input data." with --a memory to store code operating as a stream cipher; and an electronic component coupled to the memory and adapted to segment input data into random sized blocks forming a sequence of blocks, the size of each block of the sequence of blocks varying in response to changes in the input data, the electronic component adapted to further perform a stream cipher operation on the random sized blocks.--.

Claim 16, line 2: replace "involves encryption to produce cipher text" with – involves encryption using an encryption key to produce cipher text--.

Claim 17, line 1: replace "wherein the encryption logic is an integrated circuit" with –wherein the electronic component is an integrated circuit--.

Claim 18, lines 2-4: replace "processed by the encryption logic produces random-sized blocks of the input data based on the encryption key, an unique internal identifier and an output of a first non-linear function." with –processed by the electronic component produces random-sized blocks of the input data based on an encryption key, an unique internal identifier, an output of a first non-linear function and changes in the incoming plain text--.

Claim 21, line 1: replace "wherein the encryption logic to segment" with -- wherein the electronic component to segment--.

Claim 22, line 1: replace "wherein the encryption logic segments" with – wherein the electronic component segments--.

Claim 24, lines 2-3: replace "the encryption logic, enables the logic to perform" with –the electronic component, enables the electronic component to perform--

Cancel claim 25.

Cancel claim 26.

Claim 34, line 2: replace "the encryption logic" with –the electronic component--.

Double Patenting

2. The provisional double patenting rejection is withdrawn as this is the only remaining issue with the instant application, and the co-pending application (app number 09,904,962) with which the previous rejection was based on has a later filing date.

Allowable Subject Matter

3. Claims 1-24 and 30-34 are allowed.

4. The following is an examiner's statement of reasons for allowance: Applicant claims a hybrid stream cipher wherein incoming plain text is divided into variable-sized blocks based on changes of the internal state caused by variations in the incoming plain text, and the plaintext is converted into cipher text. The closest prior art, Barbir USPN 6,122,379 and Weiss 5,479,512 discloses a similar invention; both Barbir and Weiss teach a variation on concretion techniques (Barbir discloses a simultaneous compression and encryption technique that uses RLE compression and a variable step to randomize the sampling interval based on the value of a stream cipher, and Weiss discloses a compression technique using RLE then an encryption method applied to the incoming plaintext). However, in both Barbir and Weiss, the division of the plaintext into variable-sized blocks is a step of the compression part of the algorithm (RLE substitutes blocks of symbols with other blocks of symbols); in the instant application, the division into variable sized blocks are incorporated directly into the cipher to produce the ciphertext. Hence, claims 1-24 and 30-34 are allowed.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Communications Inquiry

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jung W. Kim whose telephone number is 571-272-3804. The examiner can normally be reached on M-F 9:00-5:00.

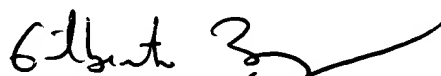
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



September 2, 2005

Jung W Kim
Examiner
Art Unit 2132



GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100